

National Cyber Alert System

[Archive](#)

Cyber Security Bulletin SB09-320

Vulnerability Summary for the Week of November 9, 2009

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System](#) (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities				
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache -- tomcat	The Windows installer for Apache Tomcat 6.0.0 through 6.0.20, 5.5.0 through 5.5.28, and possibly earlier versions uses a blank default password for the administrative user, which allows remote attackers to gain privileges.	2009-11-12	7.5	CVE-2009-3548 CONFIRM CONFIRM
apple -- mac_os_x apple -- mac_os_x_server	AFP Client in Apple Mac OS X 10.5.8 allows remote AFP servers to execute arbitrary code or cause a denial of service (memory corruption and system crash) via unspecified vectors.	2009-11-10	9.3	CVE-2009-2819 BID CONFIRM
apple -- mac_os_x apple -- mac_os_x_server	The server in DirectoryService in Apple Mac OS X 10.5.8 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via unspecified vectors.	2009-11-10	7.5	CVE-2009-2828 BID CONFIRM
apple -- mac_os_x apple -- mac_os_x_server	Buffer overflow in the UCCCompareTextDefault API in International Components for Unicode in Apple Mac OS X 10.5.8 allows context-dependent attackers to execute arbitrary code or cause a denial of service (application crash) via unspecified	2009-11-10	7.5	CVE-2009-2833 BID CONFIRM ADDE

	vectors.			APPLE
christos_zoulas -- file	Multiple integer overflows in Christos Zoulas file before 5.02 allow user-assisted remote attackers to have an unspecified impact via a malformed compound document (aka cdf) file that triggers a buffer overflow.	2009-11-10	9.3	CVE-2009-3930 MLIST
gimp -- gimp	Integer overflow in the ReadImage function in plug-ins/file-bmp/bmp-read.c in GIMP 2.6.7 might allow remote attackers to execute arbitrary code via a BMP file with crafted width and height values that trigger a heap-based buffer overflow.	2009-11-13	9.3	CVE-2009-1570 VUPEN CONFIRM
google -- chrome	Incomplete blacklist vulnerability in browser/download/download_exe.cc in Google Chrome before 3.0.195.32 allows remote attackers to force the download of certain dangerous files via a "Content-Disposition: attachment" designation, as demonstrated by (1) .mht and (2) .mhtml files, which are automatically executed by Internet Explorer 6; (3) .svg files, which are automatically executed by Safari; (4) .xml files; (5) .htt files; (6) .xsl files; (7) .xslt files; and (8) image files that are forbidden by the victim's site policy.	2009-11-12	9.3	CVE-2009-3931 VUPEN BID BUGTRAQ OSVDB MISC SECUNIA CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM
google -- chrome	The Gears plugin in Google Chrome before 3.0.195.32 allows user-assisted remote attackers to cause a denial of service (memory corruption and plugin crash) or possibly execute arbitrary code via unspecified use of the Gears SQL API, related to putting "SQL metadata into a bad state."	2009-11-12	9.3	CVE-2009-3932 VUPEN BID OSVDB SECUNIA CONFIRM CONFIRM
ibm -- advanced_management_module_firmware	Multiple unspecified vulnerabilities in the Advanced Management Module firmware before 2.50G for the IBM BladeCenter T 8720-2xx and 8730-2xx have unknown impact and attack vectors.	2009-11-12	10.0	CVE-2009-3935 VUPEN BID CONFIRM
linux -- kernel	The nfs4_proc_lock function in fs/nfs/nfs4proc.c in the NFSv4 client in the Linux kernel before 2.6.31-rc4 allows remote NFS servers to cause a denial of service (NULL pointer dereference and panic) by sending a certain response containing incorrect file attributes, which trigger attempted use of an open file that lacks NFSv4 state.	2009-11-09	7.8	CVE-2009-3726 CONFIRM
microsoft -- windows_2000 microsoft -- windows_2003_server microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp	Stack consumption vulnerability in the LDAP service in Active Directory on Microsoft Windows 2000 SP4, Server 2003 SP2, and Server 2008 Gold and SP2; Active Directory Application Mode (ADAM) on Windows XP SP2 and SP3 and Server 2003 SP2; and Active Directory Lightweight Directory Service (AD LDS) on Windows Server 2008 Gold and SP2 allows remote attackers to cause a denial of service (system hang) via a	2009-11-11	7.8	CVE-2009-1928 MS

	malformed (1) LDAP or (2) LDAPS request, aka "LSASS Recursive Stack Overflow Vulnerability."			
microsoft -- windows_server_2008 microsoft -- windows_vista	The Web Services on Devices API (WSDAPI) in Windows Vista Gold, SP1, and SP2 and Server 2008 Gold and SP2 does not properly process the headers of WSD messages, which allows remote attackers to execute arbitrary code via a crafted (1) message or (2) response, aka "Web Services on Devices API Memory Corruption Vulnerability."	2009-11-11	9.3	CVE-2009-2512 MS
microsoft -- windows_2000 microsoft -- windows_2003_server microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp	win32k.sys in the kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2 does not correctly parse font code during construction of a directory-entry table, which allows remote attackers to execute arbitrary code via a crafted Embedded OpenType (EOT) font, aka "Win32k EOT Parsing Vulnerability."	2009-11-11	9.3	CVE-2009-2514 MS
microsoft -- windows_2000	Heap-based buffer overflow in the License Logging Server in Microsoft Windows 2000 SP4 allows remote attackers to execute arbitrary code via an RPC message containing a string with a crafted length, aka "License Logging Server Heap Overflow Vulnerability."	2009-11-11	9.3	CVE-2009-2523 MS
microsoft -- compatibility_pack_word_excel_powerpoint microsoft -- excel microsoft -- excel_viewer microsoft -- office microsoft -- open_xml_file_format_converter	Microsoft Office Excel 2002 SP3 and 2003 SP3, Office 2004 and 2008 for Mac, Open XML File Format Converter for Mac, and Office Excel Viewer 2003 SP3 do not properly parse the Excel file format, which allows remote attackers to execute arbitrary code via a crafted spreadsheet, aka "Excel Cache Memory Corruption Vulnerability."	2009-11-11	9.3	CVE-2009-3127 MS
microsoft -- compatibility_pack_word_excel_powerpoint microsoft -- excel microsoft -- excel_viewer microsoft -- office microsoft -- open_xml_file_format_converter	Microsoft Office Excel 2002 SP3 and 2003 SP3, and Office Excel Viewer 2003 SP3, does not properly parse the Excel file format, which allows remote attackers to execute arbitrary code via a spreadsheet with a malformed record object, aka "Excel SxView Memory Corruption Vulnerability."	2009-11-11	9.3	CVE-2009-3128 MS
microsoft -- compatibility_pack_word_excel_powerpoint microsoft -- excel microsoft -- excel_viewer microsoft -- office microsoft -- open_xml_file_format_converter	Microsoft Office Excel 2002 SP3, 2003 SP3, and 2007 SP1 and SP2; Office 2004 and 2008 for Mac; Open XML File Format Converter for Mac; Office Excel Viewer 2003 SP3; Office Excel Viewer SP1 and SP2; and Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP1 and SP2 do not properly parse the Excel file format, which allows remote attackers to execute arbitrary code via a spreadsheet with a malformed record object, aka "Excel Featheader Record Memory Corruption Vulnerability."	2009-11-11	9.3	CVE-2009-3129 MS
microsoft -- office microsoft -- office_word	Microsoft Office Word 2002 SP3 and 2003 SP3, Office 2004 and 2008 for Mac, Open XML File Format Converter for Mac, Office Word Viewer 2003 SP3, and Office Word Viewer allow remote attackers to execute	2009-11-11	10.0	CVE-2009-3135

microsoft -- open_xml_file_format_converter	arbitrary code via a Word document with a malformed record, aka "Microsoft Office Word File Information Memory Corruption Vulnerability."			MS
microsoft -- compatibility_pack_word_excel_powerpoint microsoft -- excel microsoft -- excel_viewer microsoft -- office microsoft -- open_xml_file_format_converter	Heap-based buffer overflow in Microsoft Office Excel 2002 SP3, Office 2004 and 2008 for Mac, and Open XML File Format Converter for Mac allows remote attackers to execute arbitrary code via a spreadsheet containing a malformed Binary File Format (aka BIFF) record that triggers memory corruption, aka "Excel Document Parsing Heap Overflow Vulnerability."	2009-11-11	9.3	CVE-2009-3130 MS
microsoft -- compatibility_pack_word_excel_powerpoint microsoft -- excel microsoft -- excel_viewer microsoft -- office microsoft -- open_xml_file_format_converter	Microsoft Office Excel 2002 SP3, 2003 SP3, and 2007 SP1 and SP2; Office 2004 and 2008 for Mac; Open XML File Format Converter for Mac; Office Excel Viewer 2003 SP3; Office Excel Viewer SP1 and SP2; and Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP1 and SP2 allow remote attackers to execute arbitrary code via a spreadsheet with a crafted formula embedded in a cell, aka "Excel Formula Parsing Memory Corruption Vulnerability."	2009-11-11	9.3	CVE-2009-3131 MS
microsoft -- compatibility_pack_word_excel_powerpoint microsoft -- excel microsoft -- excel_viewer microsoft -- office microsoft -- open_xml_file_format_converter	Microsoft Office Excel 2002 SP3, 2003 SP3, and 2007 SP1 and SP2; Office 2004 and 2008 for Mac; Open XML File Format Converter for Mac; Office Excel Viewer 2003 SP3; Office Excel Viewer SP1 and SP2; and Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP1 and SP2 allow remote attackers to execute arbitrary code via a spreadsheet containing a malformed formula, related to a "pointer corruption" issue, aka "Excel Index Parsing Vulnerability."	2009-11-11	9.3	CVE-2009-3132 MS
microsoft -- compatibility_pack_word_excel_powerpoint microsoft -- excel microsoft -- excel_viewer microsoft -- office microsoft -- open_xml_file_format_converter	Microsoft Office Excel 2002 SP3, Office 2004 and 2008 for Mac, and Open XML File Format Converter for Mac allow remote attackers to execute arbitrary code via a spreadsheet containing a malformed object that triggers memory corruption, related to "loading Excel records," aka "Excel Document Parsing Memory Corruption Vulnerability."	2009-11-11	9.3	CVE-2009-3133 MS
microsoft -- compatibility_pack_word_excel_powerpoint microsoft -- excel microsoft -- excel_viewer microsoft -- office microsoft -- open_xml_file_format_converter	Microsoft Office Excel 2002 SP3, 2003 SP3, and 2007 SP1 and SP2; Office 2004 and 2008 for Mac; Open XML File Format Converter for Mac; Office Excel Viewer 2003 SP3; Office Excel Viewer SP1 and SP2; and Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP1 and SP2 do not properly parse the Excel file format, which allows remote attackers to execute arbitrary code via a spreadsheet with a malformed record object, aka "Excel Field Sanitization Vulnerability."	2009-11-11	9.3	CVE-2009-3134 MS
	Buffer overflow in pbsv.dll, as used in Soldier			

punkbuster -- punkbuster raven_software -- soldier_of_fortune_2	of Fortune II and possibly other applications when Even Balance PunkBuster 1.728 or earlier is enabled, allows remote attackers to cause a denial of service (application server crash) and possibly execute arbitrary code via a long restart packet.	2009-11-09	9.3	CVE-2009-3924 MISC
sun -- jre sun -- openjdk	Multiple unspecified vulnerabilities in the (1) X11 and (2) Win32GraphicsDevice subsystems in Sun Java SE 5.0 before Update 22 and 6 before Update 17, and OpenJDK, have unknown impact and attack vectors, related to failure to clone arrays that are returned by the getConfigurations function, aka Bug Id 6822057.	2009-11-09	7.5	CVE-2009-3879 CONFIRM CONFIRM CONFIRM
sun -- jre sun -- openjdk	Sun Java SE 5.0 before Update 22 and 6 before Update 17, and OpenJDK, does not prevent the existence of children of a resurrected ClassLoader, which allows remote attackers to gain privileges via unspecified vectors, related to an "information leak vulnerability," aka Bug Id 6636650.	2009-11-09	7.5	CVE-2009-3881 CONFIRM CONFIRM CONFIRM
sun -- jre sun -- openjdk	Multiple unspecified vulnerabilities in the Swing implementation in Sun Java SE 5.0 before Update 22 and 6 before Update 17, and OpenJDK, have unknown impact and remote attack vectors, related to "information leaks in mutable variables," aka Bug Id 6657026.	2009-11-09	7.5	CVE-2009-3882 CONFIRM CONFIRM CONFIRM
sun -- jre sun -- openjdk	Multiple unspecified vulnerabilities in the Windows Pluggable Look and Feel (PL&F) feature in the Swing implementation in Sun Java SE 5.0 before Update 22 and 6 before Update 17, and OpenJDK, have unknown impact and remote attack vectors, related to "information leaks in mutable variables," aka Bug Id 6657138.	2009-11-09	7.5	CVE-2009-3883 CONFIRM CONFIRM CONFIRM
sun -- jre	The Java Web Start implementation in Sun Java SE 6 before Update 17 does not properly handle the interaction between a signed JAR file and a JNLP (1) application or (2) applet, which has unspecified impact and attack vectors, related to a "regression," aka Bug Id 6870531.	2009-11-09	7.5	CVE-2009-3886 CONFIRM CONFIRM
sun -- virtual_desktop_infrastructure sun -- virtualbox	The VirtualBox 2.0.8 and 2.0.10 web service in Sun Virtual Desktop Infrastructure (VDI) 3.0 does not require authentication, which allows remote attackers to obtain unspecified access via vectors involving requests to an Apache HTTP Server.	2009-11-09	7.5	CVE-2009-3923 BID CONFIRM

[Back to top](#)

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	The TLS protocol, and the SSL protocol 3.0 and possibly earlier, as used in Microsoft Internet Information Services (IIS) 7.0,			

apache -- http_server gnu -- gnutls microsoft -- iis mozilla -- nss openssl -- openssl	mod_ssl in the Apache HTTP Server 2.2.14 and earlier, OpenSSL before 0.9.8l, GnuTLS 2.8.5 and earlier, Mozilla Network Security Services (NSS) 3.12.4 and earlier, and other products, does not properly associate renegotiation handshakes with an existing connection, which allows man-in-the-middle attackers to insert data into HTTPS sessions, and possibly other types of sessions protected by TLS or SSL, by sending an unauthenticated request that is processed retroactively by a server in a post-renegotiation context, related to a "plaintext injection" attack, aka the "Project Mogul" issue.	2009-11-09	6.4	CVE-2009-3555 BID CONFIRM
apple -- mac_os_x apple -- mac_os_x_server	Help Viewer in Apple Mac OS X before 10.6.2 does not use an HTTPS connection to retrieve Apple Help content from a web site, which allows man-in-the-middle attackers to send a crafted help:runscript link, and thereby execute arbitrary code, via a spoofed response.	2009-11-10	5.4	CVE-2009-2808 BID CONFIRM
apple -- mac_os_x apple -- mac_os_x_server	Launch Services in Apple Mac OS X 10.6.x before 10.6.2 recursively clears quarantine information upon opening a quarantined folder, which allows user-assisted remote attackers to execute arbitrary code via a quarantined application that does not trigger a "potentially unsafe" warning message.	2009-11-10	6.8	CVE-2009-2810 BID CONFIRM
apple -- mac_os_x_server	Adaptive Firewall in Apple Mac OS X before 10.6.2 does not properly handle invalid usernames in SSH login attempts, which makes it easier for remote attackers to obtain login access via a brute-force attack (aka dictionary attack).	2009-11-10	5.0	CVE-2009-2818 BID CONFIRM
apple -- mac_os_x apple -- mac_os_x_server	CUPS in Apple Mac OS X before 10.6.2 does not properly handle (1) HTTP headers and (2) HTML templates, which allows remote attackers to conduct cross-site scripting (XSS) attacks and HTTP response splitting attacks via vectors related to (a) the product's web interface, (b) the configuration of the print system, and (c) the titles of printed jobs.	2009-11-10	4.3	CVE-2009-2820 BID CONFIRM
apple -- mac_os_x apple -- mac_os_x_server	The Apache HTTP Server in Apple Mac OS X before 10.6.2 enables the HTTP TRACE method, which allows remote attackers to conduct cross-site scripting (XSS) attacks via unspecified web client software.	2009-11-10	4.3	CVE-2009-2823 BID CONFIRM
apple -- mac_os_x apple -- mac_os_x_server	Multiple buffer overflows in Apple Type Services (ATS) in Apple Mac OS X 10.5.8 allow remote attackers to execute arbitrary code via a crafted embedded font in a document.	2009-11-10	6.8	CVE-2009-2824 BID CONFIRM
apple -- mac_os_x apple -- mac_os_x_server	Certificate Assistant in Apple Mac OS X before 10.6.2 does not properly handle a '\o' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which might allow man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.	2009-11-10	4.3	CVE-2009-2825 BID CONFIRM
apple -- mac_os_x apple -- mac_os_x_server	Multiple integer overflows in CoreGraphics in Apple Mac OS X 10.5.8 allow remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted PDF document that triggers a heap-based buffer overflow.	2009-11-10	6.8	CVE-2009-2826 BID CONFIRM
apple -- mac_os_x apple -- mac_os_x_server	Heap-based buffer overflow in Disk Images in Apple Mac OS X 10.5.8 allows user-assisted remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted FAT filesystem on a disk image.	2009-11-10	6.8	CVE-2009-2827 BID CONFIRM
apple -- mac_os_x_server	Event Monitor in Apple Mac OS X 10.5.8 does not properly handle crafted authentication data sent to an SSH daemon, which allows remote attackers to cause a denial of service via vectors involving processing of XML log documents by other	2009-11-10	5.0	CVE-2009-2829 BID CONFIRM

	services, related to a "log injection" issue.		CONFIRM
apple -- mac_os_x apple -- mac_os_x_server	Multiple buffer overflows in Christos Zoulas file before 5.03 in Apple Mac OS X 10.6.x before 10.6.2 allow user-assisted remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted Common Document Format (CDF) file. NOTE: this might overlap CVE-2009-1515.	2009-11-10	6.8 CVE-2009-2830 BID CONFIRM APPLE
apple -- mac_os_x apple -- mac_os_x_server	Dictionary in Apple Mac OS X 10.5.8 allows remote attackers to create arbitrary files with any contents, and thereby execute arbitrary code, via crafted JavaScript, related to a "design issue."	2009-11-10	5.8 CVE-2009-2831 BID CONFIRM APPLE
apple -- mac_os_x_server	Buffer overflow in FTP Server in Apple Mac OS X before 10.6.2 allows remote attackers to execute arbitrary code or cause a denial of service (daemon crash) via a CWD command specifying a pathname in a deeply nested hierarchy of directories, related to a "CWD command line tool."	2009-11-10	5.1 CVE-2009-2832 BID CONFIRM APPLE
apple -- mac_os_x apple -- mac_os_x_server	IOKit in Apple Mac OS X before 10.6.2 allows local users to modify the firmware of a (1) USB or (2) Bluetooth keyboard via unspecified vectors.	2009-11-10	4.9 CVE-2009-2834 BID CONFIRM APPLE
apple -- mac_os_x apple -- mac_os_x_server	The kernel in Apple Mac OS X before 10.6.2 does not properly handle task state segments, which allows local users to gain privileges, cause a denial of service (system crash), or obtain sensitive information via unspecified vectors.	2009-11-10	4.6 CVE-2009-2835 BID CONFIRM APPLE
apple -- mac_os_x apple -- mac_os_x_server	Race condition in Login Window in Apple Mac OS X 10.6.x before 10.6.2, when at least one account has a blank password, allows attackers to bypass password authentication and obtain login access to an arbitrary account via unspecified vectors.	2009-11-10	6.2 CVE-2009-2836 BID CONFIRM
apple -- mac_os_x	Heap-based buffer overflow in QuickDraw Manager in Apple Mac OS X before 10.6.2 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted PICT image.	2009-11-10	6.8 CVE-2009-2837 BID CONFIRM APPLE
apple -- mac_os_x	Integer overflow in QuickLook in Apple Mac OS X 10.5.8 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted Microsoft Office document that triggers a buffer overflow.	2009-11-10	6.8 CVE-2009-2838 BID CONFIRM APPLE
apple -- mac_os_x apple -- mac_os_x_server	Screen Sharing in Apple Mac OS X 10.5.8 allows remote VNC servers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via unspecified vectors.	2009-11-10	6.8 CVE-2009-2839 BID CONFIRM APPLE
apple -- mac_os_x apple -- mac_os_x_server	Spotlight in Apple Mac OS X 10.5.8 does not properly handle temporary files, which allows local users to overwrite arbitrary files in the context of a different user's privileges via unspecified vectors.	2009-11-10	4.9 CVE-2009-2840 BID CONFIRM APPLE
apple -- safari	WebKit in Apple Safari before 4.0.4 includes certain custom HTTP headers in the OPTIONS request during cross-origin operations with preflight, which makes it easier for remote attackers to conduct cross-site request forgery (CSRF) attacks via a crafted web page.	2009-11-13	6.8 CVE-2009-2816 CONFIRM APPLE
	WebKit in Apple Safari before 4.0.4 on Mac OS X does not		

apple -- safari	perform the expected callbacks for HTML 5 media elements that have external URLs for media resources, which allows remote attackers to trigger requests to arbitrary web sites via a crafted HTML document, as demonstrated by an HTML e-mail message that uses a media element for X-Confirm-Reading-To functionality.	2009-11-13	5.0	CVE-2009-2841 CONFIRM APPLE
atheros -- ar9160-bc1a_chipset netgear -- wndap330	The Atheros wireless driver, as used in Netgear WNDAP330 Wi-Fi access point with firmware 2.1.11 and other versions before 3.0.3 on the Atheros AR9160-BC1A chipset, and other products, allows remote authenticated users to cause a denial of service (device reboot or hang) and possibly execute arbitrary code via a truncated reserved management frame.	2009-11-12	6.8	CVE-2009-0052 XF VUPEN BID BUGTRAQ OSVDB SECUNIA
chad_phillips -- userprotect	Multiple cross-site request forgery (CSRF) vulnerabilities in the User Protect module 5.x before 5.x-1.4 and 6.x before 6.x-1.3, a module for Drupal, allow remote attackers to hijack the authentication of administrators for requests that (1) delete the editing protection of a user or (2) delete a certain type of administrative-bypass rule.	2009-11-09	6.8	CVE-2009-3922 BID CONFIRM CONFIRM CONFIRM
digium -- asterisk digium -- asterisknow digium -- s800i	Asterisk Open Source 1.2.x before 1.2.35, 1.4.x before 1.4.26.3, 1.6.0.x before 1.6.0.17, and 1.6.1.x before 1.6.1.9; Business Edition A.x.x, B.x.x before B.2.5.12, C.2.x.x before C.2.4.5, and C.3.x.x before C.3.2.2; AsteriskNOW 1.5; and s800i 1.3.x before 1.3.0.5 generate different error messages depending on whether a SIP username is valid, allows remote attackers to enumerate valid usernames via multiple crafted REGISTER messages with inconsistent usernames in the URI in the To header and the Digest in the Authorization header.	2009-11-10	5.0	CVE-2009-3727 BID
ezra_barnett_gildesgame -- smartqueue_og	The Smartqueue_og module 5.x before 5.x-1.3 and 6.x before 6.x-1.0-rc3, a module for Drupal, does not verify group-node privileges in certain circumstances involving subqueue creation, which allows remote authenticated users to discover arbitrary organic group names by reading confirmation messages.	2009-11-09	4.0	CVE-2009-3921 BID CONFIRM CONFIRM CONFIRM
google -- chrome	WebKit before r50173, as used in Google Chrome before 3.0.195.32, allows remote attackers to cause a denial of service (CPU consumption) via a web page that calls the JavaScript setInterval method, which triggers an incompatibility between the WTF::currentTime and base::Time functions.	2009-11-12	5.0	CVE-2009-3933 CONFIRM OSVDB CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM
google -- chrome	The WebFrameLoaderClient::dispatchDidChangeLocationWithinPage function in src/webkit/glue/webframeclient_impl.cc in Google Chrome before 3.0.195.32 allows user-assisted remote attackers to cause a denial of service via a page-local link, related to an "empty redirect chain," as demonstrated by a message in Yahoo! Mail.	2009-11-12	4.3	CVE-2009-3934 OSVDB CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM
greg_knaddison -- s5	Cross-site scripting (XSS) vulnerability in the S5 Presentation Player module 6.x-1.x before 6.x-1.1 for Drupal allows remote attackers to inject arbitrary web script or HTML via an unspecified field that is copied to the HTML HEAD element.	2009-11-09	4.3	CVE-2009-3917 BID CONFIRM

hp -- nonstop_server	Unspecified vulnerability in Open System Services (OSS) Name Server on HP NonStop Go6.27, Go6.28, Go6.29, Go6.30, Ho6.06, Ho6.07, Ho6.08, and Jo6.03 allows remote attackers to obtain sensitive information via unknown vectors.	2009-11-13	4.0	CVE-2009-2678 HP HP
john_c_fiala -- link	Cross-site scripting (XSS) vulnerability in the "Separate title and URL" formatter in the Link module 5.x before 5.x-2.6 and 6.x before 6.x-2.7, a module for Drupal, allows remote attackers to inject arbitrary web script or HTML via the link title field.	2009-11-09	4.3	CVE-2009-3915 BID CONFIRM CONFIRM CONFIRM
karim_ratib -- zoomify	Cross-site scripting (XSS) vulnerability in the Zoomify module 5.x before 5.x-2.2 and 6.x before 6.x-1.4, a module for Drupal, allows remote attackers to inject arbitrary web script or HTML via the node title.	2009-11-09	4.3	CVE-2009-3918 BID CONFIRM CONFIRM CONFIRM
linksys -- wap4400n marvell -- 88w8361p-bem_chipset	Multiple buffer overflows in the Marvell wireless driver, as used in Linksys WAP4400N Wi-Fi access point with firmware 1.2.17 on the Marvell 88W8361P-BEM1 chipset, and other products, allow remote 802.11-authenticated users to cause a denial of service (wireless access point crash) and possibly execute arbitrary code via an association request with long (1) rates, (2) extended rates, and unspecified other information elements.	2009-11-12	6.8	CVE-2007-5475 BUGTRAQ
microsoft -- windows_2000 microsoft -- windows_2003_server microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp	win32k.sys in the kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 Gold and SP2 does not correctly validate an argument to an unspecified system call, which allows local users to gain privileges via a crafted application that triggers a NULL pointer dereference, aka "Win32k NULL Pointer Dereferencing Vulnerability."	2009-11-11	6.6	CVE-2009-1127 MS
microsoft -- windows_2000 microsoft -- windows_2003_server microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp	The Graphics Device Interface (GDI) in win32k.sys in the kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 Gold and SP2 does not properly validate user-mode input, which allows local users to gain privileges via a crafted application, aka "Win32k Insufficient Data Validation Vulnerability."	2009-11-11	6.6	CVE-2009-2513 MS
ronan_dowling -- nodehierarchy	Cross-site scripting (XSS) vulnerability in the Node Hierarchy module 5.x before 5.x-1.3 and 6.x before 6.x-1.3, a module for Drupal, allows remote attackers to inject arbitrary web script or HTML via a child node title.	2009-11-09	4.3	CVE-2009-3916 CONFIRM CONFIRM CONFIRM
sean_robertson -- crmngp	Cross-site scripting (XSS) vulnerability in the NGP COO/CWP Integration (crmngp) module 6.x before 6.x-1.12 for Drupal allows remote attackers to inject arbitrary web script or HTML via unspecified "user-supplied information."	2009-11-09	4.3	CVE-2009-3919 BID CONFIRM CONFIRM
sean_robertson -- crmngp	An administration page in the NGP COO/CWP Integration (crmngp) module 6.x before 6.x-1.12 for Drupal does not perform the expected access control, which allows remote attackers to read log information via unspecified vectors.	2009-11-09	5.0	CVE-2009-3920 BID CONFIRM CONFIRM
	Directory traversal vulnerability in the ICC_Profile.getInstance			CVE-2009-

sun -- jre sun -- openjdk	method in Java Runtime Environment (JRE) in Sun Java SE 5.0 before Update 22 and 6 before Update 17, and OpenJDK, allows remote attackers to determine the existence of local International Color Consortium (ICC) profile files via a .. (dot dot) in a pathname, aka Bug Id 6631533.	2009-11-09	5.0	CVE-2009-3728 CONFIRM CONFIRM CONFIRM
sun -- jre	Unspecified vulnerability in the TrueType font parsing functionality in Sun Java SE 5.0 before Update 22 and 6 before Update 17 allows remote attackers to cause a denial of service (application crash) via a certain test suite, aka Bug Id 6815780.	2009-11-09	5.0	CVE-2009-3729 CONFIRM CONFIRM CONFIRM
sun -- jre sun -- openjdk	The Abstract Window Toolkit (AWT) in Java Runtime Environment (JRE) in Sun Java SE 5.0 before Update 22 and 6 before Update 17, and OpenJDK, does not properly restrict the objects that may be sent to loggers, which allows attackers to obtain sensitive information via vectors related to the implementation of Component, KeyboardFocusManager, and DefaultKeyboardFocusManager, aka Bug Id 6664512.	2009-11-09	5.0	CVE-2009-3880 CONFIRM CONFIRM CONFIRM
sun -- jre sun -- openjdk	The TimeZone.getTimeZone method in Sun Java SE 5.0 before Update 22 and 6 before Update 17, and OpenJDK, allows remote attackers to determine the existence of local files via vectors related to handling of zoneinfo (aka tz) files, aka Bug Id 6824265.	2009-11-09	5.0	CVE-2009-3884 CONFIRM CONFIRM CONFIRM
sun -- jre	Sun Java SE 5.0 before Update 22 and 6 before Update 17 on Windows allows remote attackers to cause a denial of service via a BMP file containing a link to a UNC share pathname for an International Color Consortium (ICC) profile file, probably a related issue to CVE-2007-2789, aka Bug Id 6632445.	2009-11-09	5.0	CVE-2009-3885 CONFIRM CONFIRM CONFIRM
viewvc -- viewvc	Cross-site scripting (XSS) vulnerability in viewvc.py in ViewVC 1.0 before 1.0.9 and 1.1 before 1.1.2 allows remote attackers to inject arbitrary web script or HTML via the view parameter. NOTE: some of these details are obtained from third party information.	2009-11-09	4.3	CVE-2009-3618 VUPEN
viewvc -- viewvc	Unspecified vulnerability in ViewVC 1.0 before 1.0.9 and 1.1 before 1.1.2 has unknown impact and remote attack vectors related to "printing illegal parameter names and values."	2009-11-09	5.0	CVE-2009-3619 VUPEN
wolfgang_ziegler -- temporary_invitation	Cross-site scripting (XSS) vulnerability in the Temporary Invitation module 5.x before 5.x-2.3 for Drupal allows remote attackers to inject arbitrary web script or HTML via the Name field in an invitation.	2009-11-09	4.3	CVE-2009-3914 CONFIRM CONFIRM

[Back to top](#)

There were no low vulnerabilities recorded this week.

Last updated November 16, 2009

 Print This Document